IN THE UNITED STATES DISTRICT COURT OF TENNESSEE
MIDDLE DISTRICT

B.W., J.W. and A.B., individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	
	)	Case No:
v.	)	Division:
HCA HEALTHCARE INC.,	)	
Serve Registered Agent:	)	
CT Corporation System	)	
300 Montvue Rd,	)	
Knoxville, TN 37919	)	
Defendant.	)	

CLASS ACTION COMPLAINT FOR DAMAGES

COMES NOW ("Plaintiff"), individually and on behalf of all citizens who are similarly situated for her Class Action Complaint for Damages against Defendant HCA Healthcare Inc., (hereinafter "HCA"); respectfully states and alleges as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiffs, individually and on behalf of all citizens who are similarly situated (*i.e.*, the Class Members), seeking to redress Defendant's willful and reckless violations of her privacy rights. Plaintiffs and the other Class Members are patients of HCA who entrusted their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to HCA. Defendant HCA have shared Plaintiffs' PHI and PII with persons who are not authorized to have said PHI and PII. Defendant betrayed Plaintiffs' trust by failing to properly safeguard and protect their PHI and PII and publicly disclosing their PHI and PII without authorization in violation of the law.

2. This action pertains to Defendant's unauthorized disclosure of the Plaintiffs' PHI and PII that occurred sometime prior to July 10, 2023 (the "Breach").

3. Defendant disclosed Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PHI and PII.

4. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiffs' and the other Class Members' name, address, email addresses, telephone numbers, date of birth, gender, appointment dates, location and times. It is unknown if additional PHI was accessed and disclosed.

5. Defendant flagrantly disregarded Plaintiffs' and the other Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII from unauthorized disclosure. Plaintiffs' and the other Class Members' PHI and PII was improperly handled, inadequately protected, readily able to be copied by anyone with nefarious intent and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiffs' and the other Class Members' rights, both as to privacy and property.

6. Plaintiffs and the other Class Members have standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiffs and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) loss of medical expenses, and/or (iii) the additional damages set forth in detail below, which are incorporated herein by reference.

7. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate and continuing increased

risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiffs' and the other Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

8. Plaintiffs and the Class members have also suffered and are entitled to damages for the lost benefit of their bargain with Defendant HCA. Plaintiffs and members of the Class paid HCA for its services including the protection of their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiffs and the members of the Class should have received when they paid for their services, and the value of what they actually did receive; services without adequate privacy safeguards. Plaintiffs and members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiffs and the members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

9. Additionally, because of Defendant's conduct, Plaintiffs and members of the Classes have been harmed in that Defendant has breached its common law fiduciary duty of confidentiality owed to Plaintiffs and member of the Classes.

10. Accordingly, Plaintiffs and the other Classes seek redress against Defendant for breach of implied contract, outrageous conduct, common law negligence, invasion of privacy of public disclosure of private facts, negligent training and supervision, negligence *per se*, and breach of fiduciary duty of confidentiality.

11. Plaintiffs, individually and on behalf of the other Classes, seek all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

12. The Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because Defendant is a business operating in the state of Missouri.

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendant.

14. Venue is proper in the Middle District of Tennessee, pursuant to 28 U.S. Code § 1391 because the acts complained of occurred and Defendant are located in the Middle District of Tennessee.

PARTIES

15. Plaintiff B.W. is an adult residing in Jackson County, Missouri.

16. Plaintiff J.W. is an adult residing in Jackson County, Missouri.

17. Plaintiff A.B. is an adult residing in Charlotte County, Florida.

18. Defendant HCA is, upon information and belief, a nationwide company with offices all throughout the country, providing healthcare services to its patients, with their principal place

of business at HCA Healthcare, One Park Plaza, Nashville, TN 37203. HCA Inc. can be served through their registered agent, CT Corporation System, 300 Montview Rd., Knoxville, TN 37919.

BACKGROUND FACTS

19. Certain allegations are made upon information and belief.

20. Defendant HCA is a health care provider pursuant to state and federal law, providing health care and medical services to the general public, operating under common policies and procedures, throughout the United States with the central location at One Park Plaza, Nashville, TN 37203.

21. As a part of its business operations, Defendant collects and maintains PHI and PII of its patients.

22. Plaintiffs were patients of Defendant and, as a result, provided their PHI and PII to Defendant.

23. Plaintiffs entered into an implied contract with Defendant for the adequate protection of their PHI and PII.

24. Defendant is required to maintain the strictest privacy and confidentiality of Plaintiffs and the proposed Classes' medical records and other PHI and PII.

25. Defendant HCA posts its privacy practices online, at https://www.HCA.com/privacy/.

26. On or about July 5, 2023, HCA learned about the disclosure of patient information from a posting online.

27. The disclosure of the PHI and PII at issue was a result of the Defendant's inadequate safety and security protocols governing PHI and PII.

28. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiffs' and the other Class Members' name, addresses, emails, telephone numbers, date of birth, gender and patient service information such as date and location of their next medical appointment.

29. Upon information and belief, the Breach affected at least 11 million patients of Defendant.

30. As a direct and/or proximate result of Defendant's failure to properly safeguard and protect the PHI and PII of its patients, Plaintiffs' and the other Class Members' PHI and PII was stolen, compromised and wrongfully disseminated without authorization.

31. Defendant has a duty to their patients to protect them from wrongful disclosures.

32. As a business offering health care provider services, Defendant are required to train and supervise their employees regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

33. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

34. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[1] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

35. The HIPAA and HITECH rules work in conjunction with the already established State laws. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

36. The HIPAA and HITECH rules work in conjunction with the already established State laws. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

37. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

38. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

39. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

40. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

41. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

42. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[2]

43. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

44. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

45. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces

[2] 45 C.F.R. § 160.103

on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

46. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[3] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[4]

47. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

[3] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[4] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[5]

48. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

49. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

50. Defendant failed to provide proper notice to Plaintiffs of the disclosure.

51. Defendant failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

52. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiffs' and the other Class Members' compromised PHI and PII.

53. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiffs and the other Classes at an imminent, immediate and continuing increased risk of identity theft, identity fraud[6] and medical fraud.

[5] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

[6] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and

54. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *See id.*

55. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

56. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

57. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should

government fraud (theft of government services).

recognize additional harms that might arise from unanticipated uses of data."[7] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[8]

58. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *See id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *See id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *See id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *See id.* at 39.

59. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PHI and/or PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

---

[7] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[8] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

60. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

61. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

62. Defendant flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiffs' and the other Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

63. Defendant flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

64. Upon information and belief, Defendant flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

65. Defendant flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and the other Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendant's unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

66. The actual harm and adverse effects to Plaintiffs and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's above wrongful actions and/or inaction and the resulting Breach requires Plaintiffs and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiffs and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

67. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiffs and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *See id*. at 6.

68. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

69. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiffs and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i)

loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

CLASS ACTION ALLEGATIONS

70. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs brings this class action as a class action on behalf of herself and the following classes:

> **All persons residing in the United States who were patients of Defendant HCA since July 1, 2013 and whose PHI and/or PII was disclosed by Defendant to unauthorized third-parties.**
>
> **All persons residing in the United States who were residents of Missouri who were patients of Defendant HCA since July 1, 2013 and whose PHI and/or PII was disclosed by Defendant to unauthorized third-parties (the "Missouri Class").**
>
> **All persons residing in the United States who were residents of Florida who were patients of Defendant HCA since July 1, 2013 and whose PHI and/or PII was disclosed by Defendant to unauthorized third-parties (the "Florida Class").**

71. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

72. Numerosity: On information and belief, the putative Classes are comprised of tens of thousands of individuals making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

73. Commonality and Predominance: The rights of Plaintiffs and each other Class Members were violated in a virtually identical manner as a direct and/or proximate result of Defendant's 'willful, reckless and/or negligent actions and/or inaction and the resulting Breach. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendant willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the other Class Members' PHI and/or PII;

b) Whether Defendant was negligent in failing to properly safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

c) Whether Defendant owed a duty to Plaintiffs and the other Class Members to exercise reasonable care in safeguarding and protecting their PHI and/or PII;

d) Whether Defendant breached their duty to exercise reasonable care in failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

e) Whether Defendant was negligent in failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

f) Whether, by publicly disclosing Plaintiffs' and the other Class Members' PHI and/or PII without authorization, Defendant invaded their privacy; and

g) Whether Plaintiffs and the other Class Members sustained damages as a result of Defendant's failure to safeguard and protect their PHI and/or PII.

74. Adequacy: Plaintiffs and their counsel will fairly and adequately represent the interests of the other Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

75. Typicality: Plaintiffs' claims are typical of the other Class Members' claims in that Plaintiffs' claims and the other Class Members' claims all arise from Defendant's failure to properly safeguard and protect their PHI and PII.

76. Superiority and Manageability: A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and the other Class Members' claims. Plaintiffs and the other Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct.

77. Class certification, therefore, is appropriate pursuant to Federal Rule of Civil Procedure 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

78. Policies Generally Applicable to the Case: Class certification also is appropriate pursuant to Federal Rule of Civil Procedure 23 because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

79. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendant will retain the benefits of its wrongdoing despite its serious violations of the law.

80. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

81. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

82. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

COUNT I
BREACH OF IMPLIED CONTRACT

83. The preceding factual statements and allegations are incorporated herein by reference.

84. Plaintiffs and the other Class Members, as part of their agreement with Defendant HCA, provided Defendant their PHI and PII.

85. In providing such PHI and PII, Plaintiffs and the other Class Members entered into an implied contract with Defendant HCA, whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class members' PHI and PII.

86. Under the implied contract, Defendant was obligated to not only safeguard the PHI and PII, but also to provide Plaintiffs and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

87. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

88. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the other Class Members' confidential medical information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

89. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and Class members are entitled to nominal damages.

COUNT II
NEGLIGENCE

90. The preceding factual statements and allegations are incorporated herein by reference.

91. Plaintiffs bring this Count on their own behalf and on behalf of the Class and the State Subclasses (the "Classes" for the purposes of this Count).

92. Defendant owed, and continues to owe, a duty to Plaintiffs and the Classes to safeguard and protect their PHI and PII.

93. Defendant breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII.

94. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

95. Plaintiffs and the Classes entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third-parties.

96. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and the Classes could and would suffer if the PII and PHI were wrongfully disclosed.

97. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the criminal acts of a third-party.

98. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and the Classes in Defendant's possession was adequately secured and protected.

99. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients', employees', and physicians' PII and PHI that Defendant was no longer required to retain pursuant to regulations.

100. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and the Classes.

101. Defendant's duty to use reasonable security measures arose as a result of the contractual relationship that existed between Defendant and Plaintiffs and the Classes.

102. Defendant was also subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Classes.

103. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Classes was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

104. Plaintiffs and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII and PHI stored on Defendant's systems.

105. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Classes.

106. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Classes, including basic encryption techniques freely available to Defendant.

107. Plaintiffs and the Classes had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

108. Defendant were in a position to protect against the harm suffered by Plaintiffs and the Classes as a result of the Data Breach. Defendant had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third-parties.

109. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and the Classes.

110. Defendant has admitted that the PII and PHI of Plaintiffs and the Classes was wrongfully lost and disclosed to unauthorized third-persons as a result of the Data Breach.

111. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Classes by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Classes during the time the PII and PHI was within Defendant's possession or control.

112. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and the Classes in the face of increased risk of theft.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients', employees', and physicians' PII and PHI.

115. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Classes the existence and scope of the Data Breach.

116. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

117. Plaintiffs and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes are entitled to nominal damages.

118. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant,

of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

119. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes.

120. Defendant's violation of Section 5 of the FTC Act and Title II of HIPAA, including HIPAA regulations HHS has implemented pursuant to Title II, as well as the standards of conduct established by these statutes and regulations, constitutes negligence *per se.*

121. Plaintiffs and the Classes are within the class of persons that the FTC Act was intended to protect.

122. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Classes.

123. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will suffer injury, including but not limited to:

a) actual identity theft;

b) the loss of the opportunity of how their PII and PHI is used;

c) the compromise, publication, and/or theft of their PII and PHI;

d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

f) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiffs and the Classes; and

g) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Classes.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

125. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

126. Plaintiffs and the Classes are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

127. The preceding factual statements and allegations are incorporated herein by reference.

128. Plaintiffs' and the other Classes' PHI and PII was (and continues to be) sensitive and personal private information.

129. By virtue of Defendant's failure to safeguard and protect Plaintiffs' and the other Classes' PHI and PII and the resulting Breach, Defendant wrongfully disseminated Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

130. Dissemination of Plaintiffs' and the other Classes' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiffs, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

131. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation, and loss of enjoyment of life.

132. Plaintiffs and the other Classes' members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages.

133. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT IV
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

134. The preceding factual statements and allegations are incorporated herein by reference.

135. At all times relevant hereto, Defendant owed, and owes, a fiduciary duty to Plaintiffs and the proposed class pursuant to Tennessee common law, to keep Plaintiffs' medical and other PHI and PII information confidential.

136. The fiduciary duty of privacy imposed by Tennessee common law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

137. Defendant breached their fiduciary duty to Plaintiffs by disclosing Plaintiffs and the other Classes' Members PHI and PII to unauthorized third-parties.

138. As a direct result of Defendant's breach of fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential medical information, Plaintiffs and the proposed Classes' Members suffered damages.

139. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

140. Plaintiffs and the other Classes' Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages.

COUNT V
NEGLIGENT TRAINING AND SUPERVISION

141. The preceding factual statements and allegations are incorporated herein by reference.

142. At all times relevant hereto, Defendant HCA owed and owes a duty to Plaintiffs and the Classes to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

143. Defendant breached their duty to Plaintiffs and the members of the Classes by allowing its employees and agents to give access to patient medical records to an unauthorized user.

144. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

145. Plaintiffs and the other Classes members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages.

146. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VI
NEGLIGENCE *PER SE*

147. Plaintiffs incorporates by reference and re-alleges all paragraphs previously alleged herein.

148. Plaintiffs were under the medical care of the Defendant.

149. Defendant HCA are covered entities for purposes of HIPAA and HITECH.

150. Plaintiffs are members of the class HIPAA and HITECH were created to protect.

151. Plaintiffs' private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

152. The Defendant gave protected medical information to an unauthorized third-party or unauthorized third-parties without the written consent or authorization of Plaintiff.

153. The Defendant gave protected medical information to unauthorized third-parties without Plaintiffs' oral consent or written authorization.

154. The information disclosed to an unauthorized third-party or unauthorized third-parties included private health information about medical treatment.

155. Alternatively, Defendant violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiffs from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

156. As a direct result of Defendant's negligence, Plaintiffs and the Classes suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction

in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

157. Plaintiffs and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes are entitled to nominal damages.

158. As a direct result of Defendant's negligence, Plaintiffs and the Classes have a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the Defendant's wrongful acts.

159. As a direct result of Defendant's negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiffs and the Classes of, and/or protect Plaintiffs and the Classes from, being a victim of identity theft or other identity-related crimes. Plaintiffs, individually and on behalf of the Classes, seek actual damages for all monies paid to Defendant in violation of the HIPAA and HITECH. In addition, Plaintiffs seeks attorneys' fees.

COUNT VII
VIOLATIONS OF MISSOURI MERCHANDISING PRACTICES ACT, MO. REV. STAT. § 407.010 et seq.

160. The preceding factual statements and allegations are incorporated herein by reference.

161. RSMo. 407.020 prohibits the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce"…

162. An "unfair practice" is defined by Missouri law, 15 CSR 60-8.020, as any practice which:

(A) Either-

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

163. An "unfair practice is defined by Missouri law,

15 CSR 60-8.020 (1)(B) provides that an "Unfair Practice in General" is

(1) An unfair practice is any practice which –

(A) Either –

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

15 CSR 60-8.040 provides that an "Unfair Practice" is "[a]n unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in

solicitation, negotiation and performance, or in any manner fail to act in good faith." (emphasis added).

164. Plaintiffs and Defendant are "persons" within the meaning of section 407.010 (5).

165. Merchandise is defined by the MMPA, to include the providing of "services" and, therefore, encompasses Healthcare services. Healthcare services are a good.

166. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

167. Maintenance of medical records are "merchandise" within the meaning of section 407.010(4).

168. Plaintiffs' and the Class Members' goods and services purchased from Defendant were for "personal, family or household purposes" within the meaning of the Missouri Merchandising Practices Missouri Revised Statutes.

169. As set forth herein, Defendant's acts, practices and conduct violate section 407.010(1) in that, among other things, Defendant has used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offends the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in Missouri Revised Statute 407.020(1).

170. Defendant's unfair, unlawful and deceptive acts, practices and conduct include: (1) representing to its patients that it will not disclose their sensitive personal health information to an unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; and (3) failing to train personnel.

171. Defendant's conduct also violates the enabling regulations for the MMPA because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful. *See* Mo Code Regs. Ann tit. 15, Section 60-8.

172. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiffs and members of the Class have suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiffs and members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

173. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Class confidential medical information, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

174. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Class Members are entitled to nominal damages.

175. Plaintiffs, on behalf of themselves and the Class, seek actual damages for all monies paid to Defendant in violation of the MMPA. In addition, Plaintiffs seeks attorneys' fees.

COUNT VIII
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA"), FLA. STAT. § 501.201 *ET SEQ*.

176. Plaintiffs individually and on behalf of the Nationwide class, repeats and alleges the foregoing paragraphs, as if fully alleged herein.

177. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat.§ 501.204.

178. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Breach occurred through the use of the internet, an instrumentality of interstate commerce.

179. While engaged in trade or commerce, Defendant violated FDUTPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's client patients from unauthorized access and disclosure;

b. Failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendant's client patients from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Breach to Defendant's client patients in a timely and accurate manner in violation of Fla. Stat. § 501.171.

180. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

181. Defendant should have disclosed this information because they were in a superior position to know the true facts related to the defective data security.

182. Defendant's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendant's network and aggregation of Private Information.

183. The representations upon which impacted individuals (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

184. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's client patients.

185. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendant's client patients that it did not follow industry best practices for the collection, use, and storage of Private Information.

186. As a direct and proximate result of Defendant's unconscionable, unfair, and

deceptive acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages. Accordingly, Plaintiffs and Class Members are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

187. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class Members are entitled to injunctive relief, including, but not limited to:

a) Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b) Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c) Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d) Ordering that Defendant segment Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e) Ordering that Defendant purge, delete, and destroy in a reasonably secure manner Private Information not necessary for their provisions of services;

f) Ordering that Defendant conduct regular database scanning and securing checks;

g) Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

h) Ordering Defendant to meaningfully educate their current and former patients about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Defendant's current and former patients must take to protect themselves; and

i) Requiring Defendant to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to Private Information and to promptly migrate to superior or more secure alternatives.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiffs as Class Representative and appointing Plaintiffs' counsel as Lead Counsel for the Classes;

B. Declaring that Defendant breached their implied contract with Plaintiffs and Classes;

C. Declaring that Defendant negligently disclosed Plaintiffs' and the Classes' Members' PHI and PII;

D. Declaring that Defendant has invaded Plaintiffs' and Classes' Members' privacy;

E. Declaring that Defendant breached their fiduciary duty to Plaintiffs and the Classes;

F. Declaring that Defendant breached their implied contract with Plaintiffs and the Classes;

G. Declaring that Defendant HCA was negligent by negligently training and supervising its employees and agents;

H. Declaring that Defendant HCA violated the Missouri Merchandising Practices Act (MMPA);

I. Declaring that Defendant HCA violated the Florida Deceptive and Unfair Trade Practices Act;

J. Ordering Defendant to pay actual damages to Plaintiffs and the Classes;

K. Ordering Defendant to properly disseminate individualized notice of the Breach to all Classes;

L. For an Order enjoining Defendant from continuing to engage in the unlawful business practices alleged herein;

M. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs and the Classes;

N. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

O. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the other Class Members, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Respectfully submitted,

Maureen M. Brady

Maureen M. Brady MO #57800
Lucy McShane MO #57957
McSHANE & BRADY, LLC

1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

Lori G. Feldman
Michael Liskow
GEORGE FELDMAN MCDONALD, PLLC
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: (917) 983-9321
Fax: (888) 421-4173
Email: lfeldman@4-Justice.com
mliskow@4-Justice.com
eservice@4-Justice.com

ATTORNEYS FOR PLAINTIFF